## v1.1 – Changes (March 3, 2025)

- correction of multiple typos within different descriptions
- renaming local disk C into “OSDisk” (drive label)
- adding the prompt to configure NTP / NTP servers
- disabling automount
- deleting the Windows recovery partition and disabling dependent services
- expanding the partition “C” with the freed space of the deleted recovery partition
- testing the script on Windows Server 2025 (successful)
- testing the script with Veeam ONE (successful)
- adding an input prompt to let users create multiple local admins
- adding an input prompt to let users create multiple service accounts
- optimizing the script prompts on multiple lines
- adding a status bar for the main parts
- optimizing the output file

## v1.0 (Dezember 6, 2024):

Local Administrator Account:
- ask for new local admin username
- ask for password
- set "password does not expire"
- add account to local groups "Administrators" and "Remote Desktop Users"
- ask for password for built-in Administrator
- disable built-in Administrator

Account Policies:
Account Lockout Policy:
- Account lockout duration: 15min
- Account lockout threshold: 5
- Allow Administrator account lockout: Enabled
- Reset account lockout counter after: 15min

Local Policies:
User Rights Assignment:
- Access Credential Manager as trusted caller: no one
- Create a token object: no one
- Deny access to this computer: Guests
- Deny log on as batch job: Guests, Administrator (Built-In), admloc
- Deny log on as a service: Guests, Administrator (Built-In), admloc
- Deny log on locally: Guests
- Deny log on through RDP: Guests, Service Accounts
- Lock pages in memory: no one

Security Options:
- Accounts - Block Microsoft accounts: true (Users can't log on with Microsoft accounts)
- Accounts - Guest account status: disabled
- Accounts - Limit local account use of blank password to console logon: enabled
- Audit - Force audit policy subcategory settings override audit policy category settings: enabled
- Audit - Shut down system immediately if unable to log security audits: disabled
- Devices - Prevent users from installing printer drivers: enabled
- Interactive logon: Do not require CTRL+ALT+DEL: disabled
- Interactive logon: Don't display last signed-in: enabled
- Interactive logon: Machine inactivity limit: 900 (or less)
- Interactive logon: Number of previous logons to cache: 3
- Microsoft network server: Amount of idle time required before suspending session: 15min
- Network access - Let Everyone permissions apply to anonymous users: disabled
- Network access - Shares that can be accessed anonymously: none
- Network access - Sharing and security model for local accounts: classic
- Shutdown - Allow system to be shut down without having to log on': disabled
- System objects - Strengthen default permissions of internal system objects: enabled

System Services:
- Print Spooler: disabled

Windows Defender Firewall with Advanced Security:
- Windows Firewall - Domain: on
- Windows Firewall - Domain - Logging: '%SystemRoot%\System32\logfiles\firewall\domainfw.log'
- Windows Firewall - Domain - Logging size limit: 16384 or greater
- Windows Firewall - Domain - Log dropped packets: yes
- Windows Firewall - Private: on

- Windows Firewall - Private - Logging: '%SystemRoot%\System32\logfiles\firewall\privatefw.log'
- Windows Firewall - Private - Logging size limit: 16384 or greater
- Windows Firewall - Private - Log dropped packets: yes
- Windows Firewall - Public: on
- Windows Firewall - Public - Logging: '%SystemRoot%\System32\logfiles\firewall\publicfw.log'
- Windows Firewall - Public - Logging size limit: 16384 or greater
- Windows Firewall - Public - Log dropped packets: yes

Advanced Audit Policy Configuration:
- Audit credential validation: sucess and failure
- Audit Application Group Management: success and failure
- Audit Security Group Management: include success
- Audit User Account Management: success and failure
- Audit PNP activity: include success
- Audit process creation: include success
- Audit account lockout: include failure
- Audit Group membership: include success
- Audit logoff: include success
- Audit logon: success and failure
- Audit other logon/logoff events: success and failure
- Audit special logon: includesuccess
- Audit Audit policy change: include success
- Audit authentication policy change: include success
- Audit authorization policy change: include success
- Audit other policy change events: include failure
- Audit sensitive privilege use: success and failure
- Audit IPSec driver: success and failure
- Audit other system events: success and failure
- Audit security state change: success
- Audit security system exension: success
- Audit system integrity: sucess and failure

Administrative Templates (Computer):
- Prevent enabling lock screen camera: enabled
- Prevent enabling lock screen slide show: enabled
- Allow users to enable online speech recognition services: disabled
- Allone online tips: disabled
- Configure SMB v1 client driver: enabled - disable driver
- Configure VMB v1 server: disabled
- Enable certificate padding: enabled
- Enable structured exception handling overwrite protection: enabled
- WDigest authentication: disabled
- MSS - Enable automatic logon: disabled
- MSS - DisableIPSourceRouting IPv6) IP source routing protection level: enabled - Highest protection, source routing is completely disabled
- MSS - (DisableIPSourceRouting) IP source routing protection level: enabled - Highest protection, source routing is completely disabled
- MSS - (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes: disabled
- MSS - (KeepAliveTime) How often keep-alive packets are sent in milliseconds: enabled - 300,000 or 5 minutes
- MSS - (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers: enabled
- MSS - (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses: disabled
- MSS - (SafeDllSearchMode) Enable Safe DLL search mode: enabled
- MSS - (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires: enabled
- MSS - (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted: enabled
- MSS - (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted: enabled - 3
- MSS - (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning: enabled - 90% or less

- Turn off multicast name resolution: enabled
- Enable font providers: disabled
- Enable insecure guest logons: disabled

- Turn off Microsoft Peer-to-Peer networking services: enabled
- Prohibit installation and configuration of network bridge on your DNS domain network: enabled
- Prohibit use of internet connection sharing on your DNS domain network: enabled
- Require domain users to elevate when setting a network's location: enabled
- Hardened UNC paths: enabled, require mutual authentication, require integrity, require privacy for NETLOGON and SYSVOL shares

- TCPIP6 parameter "DisabledComponents": 0xff( 255)

- Configuration of wireless settings using Windows Connect Now: disabled

- Prohibit access of the Windows Connect Now wizards: enabled
- Minimize the number of simultaneous connections to the internet or a Windows domain: enabled - 3 = Prevent Wi-Fi when on Ethernet

- Allow print spooler to accept client connections: disabled
- Configure Redirection Guard: enabled
- Configure RPC connection settings: Protocol to use for outgoing RPC connections: enabled - RPC over TCP
- Configure RPC connection settings: Use authentication for outgoing RPC connections: enabled - default
- Configure RPC listener settings: Protocols to allow for incoming RPC connections: enabled - RPC over TCP
- Configure RPC listener settings: Authentication protocol to use for incomoing RPC connections: enabled - negotiate
- Configure RPC pver TCP port: enabled - 0
- Limits print driver installation to Administrators: enabled
- Point and Print restrictions - When installing drivers for a new connection: enabled - Show warning and elevation prompt

- Turn off notifications network usage: enabled

- Include command line in process creation events: enabled
- Encryption Oracle Remediation: enabled - force updated clients
- Remote host allows delegation of non-exportable credentials: enabled

- Turn on virtualization based security: enabled
- Turn on virtualization based security - select platform level: secure boot or higher
- Turn on virtualization based security - secure launch configuration: enabled

- Prevent device metadata retrieval from the internet: enabled

- Boot-Start driver initialization policy: enabled - good, unknown and bad but critical

- Configure registry policy processing - Do not apply during periodic background processing: enabled - false
- Configure registry policy processing - Process even in the Group Policy object have not changed: enabled - true
- Configure security policy processing - Do not apply during periodic background processing: enabled - false
- Configure securitypolicy processing - Process even if the Group Policy objects have not changed: enabled - true
- Continue experiences on this device: disabled
- Turn off background refresh of Group Policy: disabled

- Turn off downloading of print drivers over HTTP: enabled
- Turn off handwriting personalization data sharing: enabled
- Turn off handwriting recognition error reporting: enabled
- Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com: enabled
- Turn off Internet download for Web publishing and online ordering wizards: enabled
- Turn off printing over HTTP: enabled
- Turn off Registration if URL connection is referring to Microsoft.com: enabled
- Turn off Search Companion content file updates: enabled
- Turn off the "Order Prints: enabled
- Turn off the "Publish to Web" task for files and folders: enabled
- Turn off the Windows Messenger Customer Experience Improvement Program: enabled
- Turn off Windows Customer Experience Improvement Program: enabled
- Turn off Windows Error Reporting: enabled

- Enable password encryption: enabled
- Password Settings - Password Complexity: enabled - Large letters + small letters + numbers + special characters
- Password Settings - Password Length: enabled - 15 or more
- Post-authentication actions - actions: enabled - reset the password and logoff the managed account

- Allow Custom SSPs and APs to be loaded into LSASS: disabled
- Configures LSASS to run as a protected process: enabled

- Disallow copying of user input methods to the system account for sign-in: enabled

- Block user from showing account details on sign-in: enabled
- Do not display network selection UI: enabled
- Turn off app notifications on the lock screen: enabled
- Turn off picture password sign-in: enabled
- Turn on convenience PIN sign-in: disabled

- Allow network connectivity during connected-standby (on battery): disabled
- Allow network connectivity during connected-standby (plugged in): disabled
- Require a password when a computer wakes (on battery): enabled
- Require a password when a computer wakes (plugged in): enabled

- Configure Offer Remote Assistance: disabled
- Configure Solicited Remote Assistance: disabled

- Enable RPC Endpoint Mapper Client Authentication: enabled
- Restrict Unauthenticated RPC clients: enabled - authenticated

- Microsoft Support Diagnostic Tool - Turn on MSDT interactive communication with support provider: disabled

- Enable/Disable PerfTrack: disabled
- Turn off the advertising ID: enabled

- Enable Windows NTP Client: enabled
- Enable Windows NTP Server: disabled

- Allow Microsoft accounts to be optional: enabled
- Disallow Autoplay for non-volume devices: enabled
- Turn off Autoplay: enabled - all drives
- Set the default behavior for AutoRun: enabled - do not execute any autorun commands

- Configure enhanced anti-spoofing: enabled
- Allow Use of Camera: disabled

- Turn off cloud consumer account state content: enabled
- Turn off cloud optimized content: enabled
- Turn off Microsoft consumer experiences: enabled

- Require pin for pairing: enabled - always
- Enumerate administrator accounts on elevation: disabled

- Allow Diagnostic Data: enabled - Diagnostic data off
- Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service: enabled - disable authenticated proxy usage
- Disable OneSettings Downloads: enabled
- Do not show feedback notifications: enabled
- Enable OneSettings Auditing: enabled
- Limit Diagnostic Log Collection: enabled
- Limit Dump Collection: enabled
- Toggle user control over Insider builds: disabled

- Enable App Installer: disabled
- Enable App Installer Experimental Features: disabled
- Enable App Installer Hash Override: disabled
- Enable App Installer ms-appinstaller protocol: disabled

- Application - Control Event Log behavior when the log file reaches its maximum size: disabled
- Application - Specify the maximum log file size (KB): 32768 or greater
- Security - Control Event Log behavior when the log file reaches its maximum size: disabled
- Security - Specify the maximum log file size (KB): 196608 or greater
- Setup - Control Event Log behavior when the log file reaches its maximum size: disabled
- Setup - Specify the maximum log file size (KB): 32768 or greater
- System - Control Event Log behavior when the log file reaches its maximum size: disabled
- System - Specify the maximum log file size (KB): 32768 or greater

- Turn off Data Execution Prevention for Explorer: disabled
- Turn off heap termination on corruption: disabled
- Turn off shell protocol protected mode: disabled

- Turn off location: enabled

- Allow Message Service Cloud Sync: disabled
- Block all consumer Microsoft account user authentication: enabled

- Configure local setting override for reporting to Microsoft MAPS: disabled
- Join Microsoft MAPS: disabled

- Configure Attack Surface Reduction rules: enabled
- Prevent users and apps from accessing dangerous websites: enabled - block
- Enable file hash computation feature: enabled

- Turn off real-time protection: disabled
- Turn on behavior monitoring: enabled
- Turn on script scanning: enabled

- Configure Watson events: disabled
- Turn on e-mail scanning: enabled

- Configure detection for potentially unwanted applications: enabled - block
- Turn off Microsoft Defender AntiVirus: disabled

- Prevent the usage of OneDrive for file storage: enabled
- Turn off Push To Install service: enabled

- Restrict Remote Desktop Services users to a single Remote Desktop Services session: enabled
- Allow UI Automation redirection: disabled
- Do not allow COM port redirection: enabled
- Do not allow drive redirection: enabled
- Do not allow location redirection: enabled
- Do not allow LPT port redirection: enabled
- Do not allow supported Plug and Play device redirection: enabled
- Do not allow WebAuthn redirection: enabled

- Always prompt for password upon connection: enabled
- Require secure RPC communication: enabled
- Require use of specific security layer for remote (RDP) connections: enabled - SSL
- Require user authentication for remote connections by using Network Level Authentication: enabled
- Set client connection encryption level: enabled - high

- Set time limit for active but idle Remote Desktop Services sessions: enabled - 15 minutes or less but never 0
- Set time limit for disconnected sessions: enabled - 1 minute

- Do not delete temp folders upon exit: disabled
- Do not use temporary folders per session: disabled
- Prevent downloading of enclosures: enabled

- Allow Cloud Search: enabled . Disable cloud search
- Allow indexing of encrypted files: disabled
- Allow search highlights: disabled

- Turn off KMS Client Online AVS Validation: enabled

- Configure Windows Defender SmartScreen: enabled - warn and prevent bypass

- Allow suggested apps in Windows Ink Workspace: disabled
- Allow Windows Ink Workspace: enable - disabled

- Allow user control over installs: disabled
- Always install with elevated privileges: disabled
- Prevent Internet Explorer security prompt for Windows Installer scripts: disabled

- Enable MPR notifications for the system: disabled
- Sign-in and lock last interactive user automatically after a restart: disabled

- Turn on PowerShell Script Block Logging: enabled
- Turn on PowerShell Transcription: enabled

WinRM Client:
- Allow Basic authentication: disabled
- Allow unencrypted traffic: disabled
- Disallow Digest authentication: enabled

WinRM Service:
- Allow Basic authentication: disabled
- Allow remote server management through WinRM: disabled
- Allow unencrypted traffic: disabled
- Disallow WinRM from storing RunAs credentials: enabled

Windows Remote Shell:
- Allow Remote Shell Access: disabled

App and browser protection:
- Prevent users from modifying settings: enabled

Legacy Policies:
- No auto-restart with logged on users for scheduled automatic updates installations: disabled

Manage updates offered from Windows Update (formerly Defer Windows Updates and Windows Update for Business):
- Manage preview builds: disabled
- Select when Preview Builds and Feature Updates are received: enabled - 180 or more days
- Select when Quality Updates are received: enabled - 0 days